IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

NORTH ALABAMA EDUCATORS CREDIT UNION, on behalf of itself and all others similarly situated,	)	
Plaintiff,	)	**CIVIL ACTION NO.:** _____
v.	)	**JURY TRIAL DEMANDED**
ARBY'S RESTAURANT GROUP, INC.,	)	
Defendant.	)	

CLASS ACTION COMPLAINT

North Alabama Educators Credit Union ("NAECU" or "Plaintiff"), individually and on behalf of all others similarly situated, alleges the following against Arby's Restaurant Group, Inc. ("Arby's" or "Defendant"):

SUMMARY OF ACTION

1. Plaintiff brings this class action on its own behalf and on behalf of other financial institutions that suffered, and continue to suffer, financial losses as a direct result of Arby's conscious failure to take adequate and reasonable measures to protect its point-of-sale ("POS") network and computer systems.

2. Despite repeated warnings from security experts about the risk of POS data breaches and numerous data breaches of other retailers, such as Wendy's, Home Depot, Target, Dairy Queen, and Kmart, over the past few years, Arby's failed to comply with industry standards and its statutory and common law duties to protect the Payment Card Data (as defined in ¶3) of its customers.

3. Between October 25, 2016 and January 19, 2017, hundreds of thousands, if not millions, of credit and debit cards issued by financial institutions, including Plaintiff, were compromised due to Arby's severely inadequate security practices. Arby's actions and omissions left highly sensitive Payment Card Data of the Plaintiff's customers exposed and accessible for hackers to steal for nearly three months. "Payment Card Data" includes, but is not limited to, the cardholder name, credit or debit card number, expiration date, cardholder verification value, and service code. As a result, NAECU and other financial institutions incurred significant financial losses including, but not limited to, costs to cancel and reissue compromised payment cards, costs to reimburse their customers for fraudulent charges, and costs to investigate fraudulent charges.

4. Plaintiff seeks to recover damages as well as equitable relief on behalf of itself and all other similarly situated financial institutions in the United States.

JURISDICTION AND VENUE

5. This Court has original jurisdiction over this action pursuant to the Class Action Fairness Act, 28 U.S.C § 1332(d). The matter in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, at least one member of the proposed Class is of diverse citizenship from the Defendant, and there are more than 100 putative class members.

6. This Court has personal jurisdiction over Defendant because it maintains a principal place of business in the state of Georgia, regularly conducts business in Georgia, and has sufficient minimum contacts in Georgia.

7. Venue is proper under 18 U.S.C. § 1391(b) because Defendant's principal place of business is in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

PARTIES

8. Plaintiff NAECU is an Alabama-chartered credit union with its principal place of business in Huntsville, Alabama. NAECU operates branches throughout North Alabama. As a credit union, Plaintiff is a cooperative whose members are consumers.

9. NAECU is a MasterCard payment card issuer and has suffered financial losses due to the Arby's data breach. On or about February 8, 2017, NAECU received an Account Data Compromise alert from MasterCard and a news bulletin from the League of Southeastern Credit Unions.

10. Defendant Arby's is a Delaware corporation with its principal place of business located in Atlanta, Georgia.

11. Arby's is engaged in the business of operating, developing, and franchising a system of quick-service restaurants. Arby's accepts payment for its goods and services through a POS network. Consumers swipe payment cards, which are issued by Plaintiff and the proposed Class, at Arby's POS terminals to effectuate payment for Arby's goods and services.

STATEMENT OF FACTS

12. Recently, financial institutions have experienced an unprecedented number of Compromised Account Management System ("CAMS") alerts on their members' accounts from VISA and Account Data Compromise ("ADC") alerts on their members' accounts from MasterCard. CAMS and ADC alerts typically are issued by VISA and MasterCard when there is some event that jeopardizes the security of a financial institution's customers' accounts.

13. Numerous financial institutions have traced the large number of alerts issued for their customers' accounts and discovered a common denominator: Arby's.

14. On or about February 7, 2017, VISA issued a CAMS alert estimating that the "Exposure Window" for the breach of Arby's computer systems was between October 25, 2016 and January 19, 2017. The CAMS alert further indicates that both Track 1 and Track 2 data may have been compromised in the data breach. Track 1 and Track 2 data normally includes credit and debit card information such as cardholder name, primary account number, expiration date, and in certain instances PIN number.

15. On or about February 8, 2017, MasterCard issued an ADC alert estimating that the "At-Risk Time Frame" for the breach of Arby's computer systems was between October 28, 2016 and January 17, 2017. In other words, Arby's security was so deficient that it was unaware that hackers were accessing its system and stealing cardholder data for over 80 days.

16. On or about February 9, 2017, Arby's provided a very brief statement to an industry-security expert acknowledging that malware had infected its POS network.

17. On or about February 9, 2017, Arby's added a notification regarding the data breach to its own corporate website, acknowledging that malware had in fact been present on the payment card systems at many of its stores. The notification directs Arby's customers to monitor payment card accounts and report any unauthorized activity to the bank that issued the card.

18. Unlike other retailers who have experienced data breaches, Arby's has yet to release any specific details about the data breach, such as the number and locations of impacted stores.

19. The breach of Arby's data systems occurred through Arby's POS network, where hackers installed malware that allowed them to steal payment card data from remote locations as each card was swiped for payment.

20. Arby's disregarded the security of its POS network and the potential danger of a data breach and failed to put in place reasonable systems and procedures to prevent the harm that its actions have caused, enabling the data breach.

21. Arby's knew or should have known the danger of not safeguarding its POS network given recent high-profile data breaches of retailers that occurred in the very same manner.

22. Despite this knowledge, Arby's acted unreasonably and failed to adequately and reasonably protect its customers' Payment Card Data.

23. Arby's failure is particularly egregious because various state and federal statutes obligate Arby's to act reasonably to protect the Payment Card Data of the members of NAECU and the members and customers of the proposed Class.

24. First, the payment card industry (MasterCard, VISA, Discover, and American Express), long before the breach of Arby's data systems, issued Card Operating Regulations that: (1) are binding on Arby's; (2) required Arby's to protect Payment Card Data and prevent its unauthorized disclosure; (3) prohibited Arby's from storing such data, even in encrypted form, longer than necessary to process the transaction; and (4) mandated that Arby's comply with industry standards.

25. Second, the payment card industry set rules requiring all businesses, including Arby's, to upgrade to new card readers that accept EMV chips. EMV chip technology uses imbedded computer chips instead of magnetic stripes to store Payment Card Data. Unlike magnetic-stripe cards that use static data (the card information never changes), EMV cards use dynamic data. Every time an EMV card is used, the chip creates a unique transaction code that cannot be used again.

Such technology greatly increases payment card security because, if an EMV chip's information is stolen, the unique number cannot be used by the hackers, making it much more difficult for criminals to profit from what is stolen.

26. The deadline for businesses to transition their systems from magnetic-stripe to EMV technology was October 1, 2015. Upon information and belief, Arby's failed to meet this deadline.

27. Under the Card Operating Regulations that are binding on Arby's, businesses accepting payment cards, but not meeting the October 1, 2015 deadline, are liable for damages resulting from any data breaches.

28. Third, the Payment Card Industry Security Standards Council promulgates minimum standards applicable to all organizations that store, process, or transmit payment card data. These standards are known as the Payment Card Industry Data Security Standard ("PCI DSS"). PCI DSS is the industry standard governing the security of Payment Card Data, setting the minimum for what must be done, not the maximum.

29. PCI DSS 3.1, the version of the standards in effect at the time of the Arby's data breach, sets forth detailed and comprehensive requirements that must be followed to meet twelve "high-level" mandates. Among other things, PCI DSS

required Defendant, at a minimum, to: properly secure payment card data; not store cardholder data beyond the time necessary to authorize a transaction; maintain up-to-date antivirus software and a proper firewall; restrict access to payment card data on a need-to-know basis; establish a process to identify and timely fix security vulnerabilities; assign unique identification numbers to each individual with access to its systems; and, encrypt payment card data at the point of sale.

30. Fourth, according the Federal Trade Commission ("FTC"), the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45.

31. In 2007, the FTC published guidelines establishing reasonable data security practices for businesses. The guidelines state that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems. The guidelines also recommend that businesses consider using an intrusion detection

system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating that someone may be trying to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

32. The FTC also has published a document entitled "FTC Facts for Business," which highlights the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.

33. The FTC has issued orders against businesses that failed to employ reasonable measures to secure customer data. These orders provide further guidance to businesses with regard to their data security obligations.

34. Fifth, multiple states have enacted data breach statutes requiring merchants to use reasonable care to guard against unauthorized access to consumer information, such as California Civil Code § 1798.81.5(b) and Wash. Rev. Code § 19.255, or that otherwise impose data security obligations on merchants, such as Minnesota Plastic Card Security Act, Minn. Stat. § 325E.64. States have also adopted unfair and deceptive trade practices acts, which prohibit unfair trade practices, including the failure to employ reasonable security processes to protect

Payment Card Data. Moreover, most states have enacted statutes requiring merchants to provide notice if their data security systems are breached. These statutes, implicitly or explicitly, support the use of reasonable data security practices and reflect the public policy of protecting sensitive customer data.

35. Arby's failure to employ practices and procedures reasonably capable of securing the Payment Card Data of Plaintiff's customers and of the customers of the proposed Class violated all of these statutory and industry-imposed obligations and caused substantial damages to Plaintiff and the proposed Class.

36. Indeed, the fact that Payment Card Date was left exposed for over 80 days, while Arby's continuously failed to detect this vulnerability, demonstrates the complete lack of security and safeguards with respect to Payment Card Data.

37. Plaintiff and the proposed Class were required to act immediately to mitigate the massive fraudulent transactions being made on payment cards that they had issued, while simultaneously taking steps to prevent future fraud. Consumers are ultimately protected from most fraud losses, but Plaintiff and the proposed Class members are not. Financial institutions bear primary responsibility for reimbursing members for fraudulent charges on the payment cards they issue.

38. As a result of the Arby's data breach, NAECU and the proposed Class have been forced to cancel and reissue payment cards, change or close accounts, notify members that their cards were compromised, investigate claims of fraudulent activity, refund fraudulent charges, increase fraud monitoring on potentially impacted accounts, and take other steps to protect themselves and their members. NAECU and the proposed Class have also lost interest and transaction fees due to reduced card usage.

39. The financial damages suffered by Plaintiff and the proposed Class are massive and continue to increase.

40. Arby's data breach caused NAECU to incur significant costs associated with, among other things, notifying members of issues related to the data breach, closing out and opening new customer/member accounts, reissuing members' cards, and/or refunding members' losses resulting from the unauthorized use of their accounts.

CLASS ALLEGATIONS

41. Plaintiff brings this action on behalf of itself and all other similarly situated financial institutions pursuant to Rule 23(a), (b)(2) and (b)(3) of the

Federal Rules of Civil Procedure. Plaintiff seeks certification of the following proposed Class (the "Class"), defined as:

> All banks, credit unions, financial institutions, and other entities in the United States (including its Territories and the District of Columbia) that issued payment cards (including debit or credit cards) used by consumers to make purchases from Arby's while malware was installed on its payment card systems.

42. Excluded from the proposed Class are Defendant and its subsidiaries and affiliates; all employees of Defendant; all persons who make a timely election to be excluded from the proposed Class; government entities; the judge to whom this case is assigned, his/her immediate family, and his/her court staff.

43. Numerosity: All requirements of Fed. R. Civ. P. 23(a)(l) are satisfied. The members of the proposed Class are so numerous and geographically dispersed that individual joinder of all proposed Class members is impracticable. While Plaintiff is informed and believes that there are thousands of members of the proposed Class, the precise number of class members is unknown to Plaintiff. Class members may be identified through objective means. Class members may be notified of the pendency of this action by recognized, Court-approved notice

dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

44. Commonality and Predominance: All requirements of Fed. R. Civ. P. 23(a)(2) and 23(b)(3)'s predominance requirement are satisfied. This action involves common questions of law and fact, which predominate over any questions affecting individual class members, including, without limitation:

a. Whether Defendant engaged in the misconduct alleged;

b. Whether Defendant owed a duty to Plaintiff and the class members and whether Defendant violated that duty;

c. Whether Plaintiff and the Class members were injured and suffered damages or other ascertainable loss as a result of Defendant's conduct; and

d. Whether Plaintiff and the Class members are entitled to relief and the measure of such relief.

45. Typicality: All requirements of Fed. R. Civ. P. 23(a)(3) are satisfied. Plaintiff is a member of the Class, having issued payment cards that were compromised in the data breach of Defendant’s payment card systems. Plaintiff’s

claims are typical of the other Class members' claims because, among other things, all Class members were comparably injured through Defendant's uniform conduct.

46. Adequacy: All requirements of Fed. R. Civ. P. 23(a)(4) are satisfied. Plaintiff is an adequate Class representative because it is a member of the Class and its interests do not conflict with the interests of the other members of the Class that it seeks to represent. Plaintiff is committed to pursuing this matter for the Class with the Class's collective best interests in mind. Plaintiff has retained counsel competent and experienced in complex class action litigation of this type, and Plaintiff intends to prosecute this action vigorously. Plaintiff and its counsel will fairly and adequately protect the Class's interests.

47. Superiority: The superiority requirement of Fed. R. Civ. P. 23(b)(3) is satisfied. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiff and the other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be impracticable for members of the Class to individually seek redress for Defendant's wrongful conduct. Even if

Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

48. Injunctive and Declaratory Relief: All requirements of Fed. R. Civ. P. 23(b)(2) are satisfied. Defendant, through its uniform conduct, acted or refused to act on grounds generally applicable to the class as a whole, making injunctive and declaratory relief appropriate to the class as a whole.

COUNT I

Negligence

49. Plaintiff repeats and re-alleges the factual allegations contained in every preceding paragraph as if fully set forth herein.

50. Arby's owed a duty to Plaintiff and the members of the proposed Class to take reasonable care to protect Payment Card Data, and to timely notify Plaintiff and the proposed Class in the event of a data breach. This duty arises from multiple sources.

51. At common law, Defendant owed a duty to Plaintiff and the proposed Class because it was foreseeable that Defendant's data systems and the Payment Card Data those data systems processed would be targeted by hackers. It also was foreseeable that such hackers would extract Payment Card Data from Defendant's systems and misuse that information to the detriment of Plaintiff and the Class members, and that Plaintiff and the Class would be forced to mitigate such fraud or such potential fraud by cancelling and reissuing payment cards to their members and reimbursing their members for fraud losses.

52. Defendant's common law duty also arises from the special relationship that existed between Defendant and Plaintiff and the Class. Plaintiff and the Class entrusted Defendant with the Payment Card Data contained on the payment cards Plaintiff and the Class issued to their members. Defendant, as the holder and processor of that information, was the only party who realistically could ensure that its data systems were sufficient to protect the Payment Card Data it was entrusted to process and/or hold.

53. In addition to the common law, Section 5 of the FTCA, 15 U.S.C. § 45, further required Defendant to take reasonable measures to protect the Payment Card Data. Section 5 prohibits unfair practices in or affecting

commerce, which requires and obligates Defendant to take reasonable measures to protect any Payment Card Data Defendant may hold or process. The FTC publications and data security breach orders described above further form the basis of Defendant's duty. In addition, individual states have enacted statutes based upon the FTCA that also created a duty.

54. Defendant also is obligated to perform its business operations in accordance with industry standards, including the PCI DSS, to which Defendant is bound. The industry standards create yet another source of obligations that mandate Defendant to exercise reasonable care with respect to Plaintiff and the Class.

55. Defendant, by its actions and inactions, breached its duties to Plaintiff and the Class. Specifically, Defendant failed to act reasonably in protecting the Payment Card Data of the customers of Plaintiff and the Class, and did not have reasonably adequate systems, procedures and personnel in place to prevent the disclosure and theft of the Payment Card Data of the customers of Plaintiff and the Class.

56. Upon information and belief, the specific negligent acts and omissions committed by Defendant include, but are not limited to, some or all of the following:

a. failure to delete cardholder information after the time period necessary to authorize the transaction;

b. failure to employ systems to protect against malware;

c. failure to regularly update its antivirus software;

d. failure to maintain an adequate firewall;

e. failure to track and monitor access to its network and Payment Card Data;

f. failure to limit access to its network and to Payment Card Data to those with a valid purpose;

g. failure to encrypt Payment Card Data at the point-of-sale;

h. failure to transition to the use of EMV technology;

i. failure to conduct frequent audit log reviews and vulnerability scans and remedy problems that were found;

j. failure to assign a unique ID to each individual with access to its systems;

k. failure to automate the assessment of technical controls and security configuration standards;

l. failure to adequately staff and fund its data security operation;

m. failure to use due care in hiring, promoting, and supervising those responsible for its data security operations;

n. failure to recognize red flags signaling that Defendant's systems were inadequate, and that as a result, the potential for a massive data breach was increasingly likely;

o. failure to recognize that hackers were stealing Customer Data from its network while the data breach was taking place; and

p. failure to disclose the data breach in a timely manner.

57. In connection with the conduct described above, Defendant acted wantonly, recklessly, and with complete disregard for the consequences.

58. As a direct and proximate result of Defendant's conduct, Plaintiff and the Class have suffered and continue to suffer injury, including but not limited to cancelling and reissuing payment cards, changing or closing accounts, notifying members that their cards were compromised, investigating claims of fraudulent activity, refunding fraudulent charges, increasing fraud monitoring on potentially

impacted accounts, and taking other steps to protect themselves and their members. They also lost interest and transaction fees due to reduced card usage resulting from the breach, and the cards they issued (and the corresponding account numbers) were rendered worthless.

59. Because no statutes of other states are implicated, Georgia common law applies to Plaintiff and the Class's negligence claim.

COUNT II

Negligence *Per Se*

60. Plaintiff repeats and re-alleges the factual allegations contained in every preceding paragraph as if fully set forth herein.

61. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits "unfair…practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by retailers, restaurants and other businesses such as Defendant of failing to use reasonable measures to protect Payment Card Data. The FTC publications and orders described above also form the basis of Defendant's duty.

62. Defendant violated Section 5 of the FTCA (and similar state statutes) by failing to use reasonable measures to protect cardholder data and not complying

with applicable industry standards, including PCI DSS, as previously described in detail. Defendant's conduct was particularly unreasonable given the nature and amount of Payment Card Data it obtained, processed, and/or stored and the foreseeable consequences of a data breach at a national retailer, including, specifically, the immense damages that would result to consumers and financial institutions.

63. Defendant's violation of Section 5 of the FTCA (and similar state statutes) constitutes negligence per se.

64. Plaintiff and the proposed Class are within the class of persons Section 5 of the FTCA (and similar state statutes) was intended to protect, as they are engaged in trade and commerce and bear primary responsibility for reimbursing consumers for fraud losses. Moreover, Plaintiff and many class members are credit unions, which are organized as cooperatives whose members are consumers.

65. Moreover, the harm that has occurred is the type of harm the FTCA (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses that, as a result of their

failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and the proposed Class.

66. As a direct and proximate result of Defendant's negligence per se, the Plaintiff and the Class have suffered and continue to suffer injury, including, but not limited to, the expense of cancelling and reissuing payment cards, changing or closing accounts, notifying members that their cards were compromised, investigating claims of fraudulent activity, refunding fraudulent charges, increasing fraud monitoring on potentially impacted accounts, and taking other steps to protect themselves and their members. They also lost interest and transaction fees due to reduced card usage resulting from the breach, and the cards they issued (and the corresponding account numbers) were rendered worthless.

67. Because no statutes of other states are implicated, Georgia common law applies to Plaintiff and the Class's negligence *per se* claim.

COUNT III

Declaratory and Injunctive Relief

68. Plaintiff repeats and re-alleges the allegations contained in every preceding paragraph as if fully set forth herein.

69. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and granting further necessary relief. Furthermore, the Court has broad authority to restrain tortious acts that violate the terms of the federal and state statutes described herein.

70. An actual controversy has arisen in the wake of the data breach at issue regarding Defendant's common law and other duties to act reasonably with respect to safeguarding the Payment Card Data of the members of Plaintiff and the members and customers of the Class. Defendant's actions in this respect were inadequate, and Defendant denies such allegations. Additionally, Plaintiff continues to suffer injury as additional fraudulent and other illegal charges are being made on payment cards Plaintiff and the Class have issued.

71. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owed and continues to owe a legal duty to secure customers' Payment Card Data, specifically including information pertaining to credit and debit cards used by persons who made purchases at Defendant's restaurants and to notify

financial institutions of a data breach under the common law, Section 5 of the FTCA, Card Operating Regulations, PCI DSS standards, its commitments, and various state statutes;

b. Defendant breached this legal duty by failing to employ reasonable measures to secure customers' Payment Card Data;

c. Defendant's breach of its legal duty proximately caused the data breach; and

d. Banks, credit unions, and other financial institutions that reissued payment cards and were forced to pay for fraudulent transactions as a result of the Defendant's data breach were damaged and are legally entitled to recover the costs they incurred from Defendant.

72. Plaintiff and the Class are also entitled to corresponding injunctive relief requiring Defendant to employ adequate security protocols, consistent with industry standards, to protect Plaintiff's and the Class's customers' Payment Card Data. Specifically, this injunction should, among other things, require Defendant to:

a. utilize industry standard encryption to encrypt transmission of cardholder data at the point-of-sale and at all other times;

b. implement encryption keys in accordance with industry standards;

c. implement EMV technology;

d. consistent with industry standards, engage third-party auditors to test its systems for weakness and upgrade any such weakness found;

e. audit, test, and train its data security personnel regarding new or modified procedures and how to respond appropriately to a data breach;

f. regularly test its systems for security vulnerabilities, consistent with industry standards;

g. comply with all PCI DSS standards pertaining to the security of its customers' Payment Card Data; and

h. install all upgrades recommended by manufacturers of security software and firewalls used by Defendant.

73. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach of Defendant's data systems. The risk of another such data breach is real, immediate, and substantial. If another breach of Defendant's data systems occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

74. The hardship to Plaintiff and the Class if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Among other things, if Defendant suffers another massive data breach, Plaintiff and the Class will likely incur hundreds of millions of dollars in damage. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

75. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach, thus eliminating the injuries that would result to

Plaintiff, the Class, and the millions of consumers whose confidential information would be compromised.

PRAYER FOR RELIEF

76. Wherefore, Plaintiff, on behalf of itself and on behalf of the proposed Class, requests that this Court award relief against Defendant as follows:

a. Providing a jury trial for all issues so triable;

b. Entering an order certifying the class and designating Plaintiff as the Class Representative and its counsel as Class Counsel;

c. Awarding Plaintiff and the Class members damages with pre-judgment and post-judgment interest;

d. Entering a declaratory judgment in favor of Plaintiff and the Class as described above;

e. Granting Plaintiff and the Class the injunctive relief requested above;

f. Awarding attorneys' fees and costs; and

g. Awarding such other and further relief as the Court may deem necessary or appropriate.

JURY DEMAND

Plaintiff demands a trial by jury on all issues so triable.

Dated: February 23, 2017

Respectfully submitted,

/s/ N. Kirkland Pope
N. Kirkland Pope
GA Bar No. 584255
POPE McGLAMRY, P.C.
3391 Peachtree Road, NE, Suite 300
Atlanta, GA 30326
Tel: (404) 523-7706
Fax (404) 524-1648
E-mail: efile@pmkm.com

Chris T. Hellums (ASB-5583-L73C)
(Pro Hac Application to be Submitted)
Jonathan S. Mann (ASB-1083-A36M)
(Pro Hac Application to be Submitted)
PITTMAN DUTTON & HELLUMS, P.C.
2001 Park Place North
1100 Park Place Tower
Birmingham, AL 35203
Tel: (205) 322-8880
Fax: (205) 328-2711
Email: PDH-efiling@pittmandutton.com

Attorneys for Plaintiff